Technical Cybersecurity

Attack Surfaces

Attack surfaces and vectors are related, but how?

Surfaces & Vectors

A Surface is a collection of *Vectors*

- A single system? All the vectors compose the surface
- It gets complicated with aggregated systems

Attack surfaces don't change

- …but the **exposed** attack surface does
- …and the **exposed** surface is all you can attack

All Vectors Not Created Equal!

THE SURFACE IS ALL VECTORS

- …but they may not be all **accessible**
- …they may not be all **exploitable**

STILL POSSIBLE ROUTES OF ACCESS

- A vector may not be exploitable now, but it might be tomorrow, or the day after
- Developers always need to keep the attack surface as small as possible

Case: Smart Bulb

Let’s look at a smart bulb, a typical and common consumer-centric IoT system. Phillips is a common vendor, as is TP-Link. This hypothetical bulb has a network interface, and runs an outdated version of Linux with the Das U-Boot bootloader.

Case: Smart Bulb

Following the instructions, the bulb has a Bluetooth interface we can use to configure the device with an app provided by the manufacturer.

Vector 0: Bluetooth Interface

- We can attach to it and exchange data with the device directly from the supplied smartphone app. Depending on the app, this is a possible attack vector.

Case: Smart Bulb

After we've configured the bulb, we connect it to a local WiFi network. We scan the device with **nmap** and gather some interesting information.

Vector 1: HTTP Server

- The bulb runs an HTTP server on port 80. It isn't encrypted or secured, and doesn't use any kind of authentication. It provides status information.

Vector 2: SSH Daemon

- SSH runs on port 22.

Vector 3: Misc Ports

- The device has miscellaneous ports open, perhaps for proprietary communication.

Case: Smart Bulb

After attaching the device to our WiFi network, we monitor traffic.

VECTOR 4: DNS

- The device uses DNS to resolve hostnames. The DNS server seems to be set via DHCP.

VECTOR 5: HTTP TRAFFIC

- The device is connecting to remote HTTP servers.

VECTOR 6: OTHER TCP/IP TRAFFIC

- The device is also exchanging TCP/IP traffic on other ports.

Case: Smart Bulb

The bulb is plugged into a lamp. The smartphone app also gives us the ability to configure automatic firmware updates.

VECTOR 7: POWER INTERFACE

- The bulb screws into a standard lamp socket.

VECTOR 8: UPDATES

- Firmware can be loaded on the device automatically.

Vulnerabilities & Exploits

The Exploit Database

- https://www.exploit-db.com

The National Vulnerability Database

- https://nvd.nist.gov

Common Vulnerabilities and Exposures

- https://cve.mitre.org

Metasploit, articles, and more!

Let’s start with this.
Next up, analysis!